# Regtech Adoption Practice Guide

## Issue #2: Anti-Money Laundering/ Counter-Financing of Terrorism

July 2021

HONG KONG MONETARY AUTHORITY
香港金融管理局

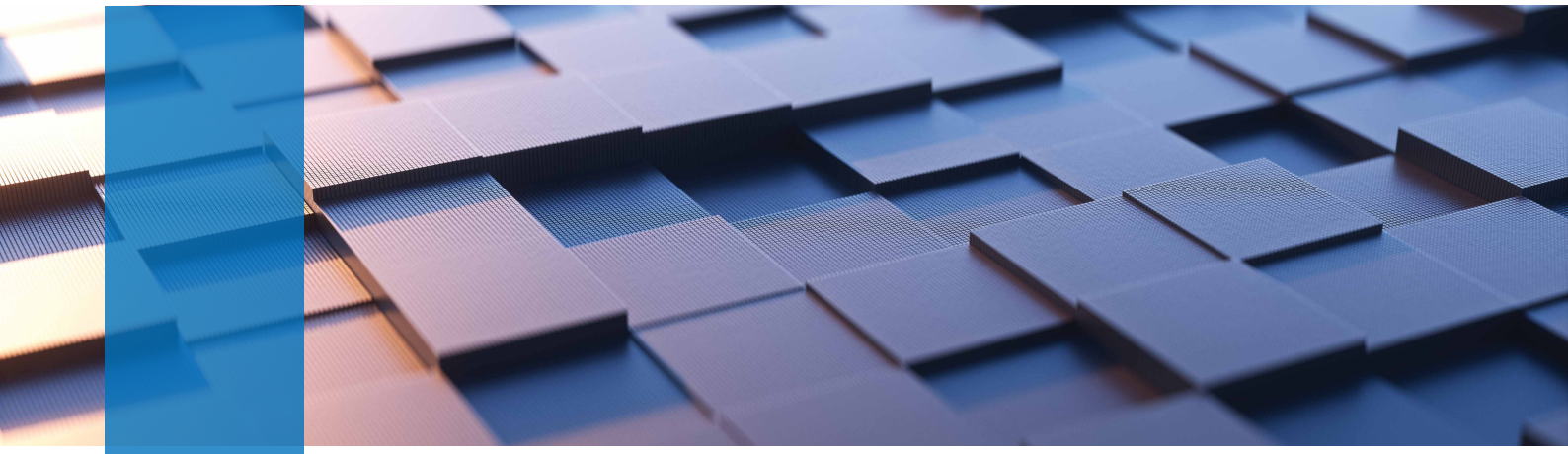
KPMG

**Disclaimer**

Regtech Adoption Practice Guide is a publication published by the Hong Kong Monetary Authority (HKMA). It should be noted that the sole purpose of this publication is to provide Authorized Institutions (banks) with information on the latest regulatory technology (Regtech) developments. The HKMA does not endorse any use cases, solutions and/or implementation guidance described in this adoption practice guide. If a bank intends to adopt a particular solution or implementation, it should undertake its own due diligence to ensure that the technology or approach is suitable for its circumstances.


13 H
70F
5

# Contents



# 01 Introduction

## 1.1 Background

**The value of Regtech in banking is coming to the fore in Hong Kong, offering clear benefits to banks, customers and regulators. In November 2020, the HKMA released a two-year roadmap to promote Regtech adoption in Hong Kong, as laid out in a White Paper titled "Transforming Risk Management and Compliance: Harnessing the Power of Regtech".[1] The White Paper identifies 16 recommendations across five core areas to accelerate the further adoption of Regtech in Hong Kong.**

The White Paper acknowledges that since 2019, the HKMA has published a series of "Regtech Watch" newsletters, introducing banks to Regtech use cases on the adoption of innovative technology to enhance risk management and regulatory compliance. The banks interviewed for the White Paper cited these newsletters as a valuable source of information and guidance, especially the actual or potential Regtech use cases that have been rolled out or are being explored in Hong Kong or globally.

The White Paper identified 26 specific application areas of Regtech that can benefit banks. There are significant opportunities and a strong desire from the industry for the HKMA to develop and issue "Regtech Adoption Practice Guides" around these application areas.

As a successor, this Regtech Adoption Practice Guide (Guide) series builds on the "Regtech Watch" newsletters to include common industry challenges, guidance on implementation and examples of what others have done successfully to overcome adoption barriers. The Guides are to supplement other ongoing HKMA initiatives such as the Banking Made Easy initiative, Fintech Supervisory Sandbox and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help to further drive Regtech adoption in Hong Kong.

Regtech solutions have emerged to improve the effectiveness and efficiency of risk management and compliance activities through harnessing new technologies such as Cloud, Artificial Intelligence, and Blockchain. The first Guide in this series outlined the benefits of Cloud-based Regtech solutions. The second Guide of the series focuses on Regtech solutions applied to "Anti-Money Laundering/ Counter-Financing of Terrorism" (AML/CFT) specifically for the ongoing monitoring of customers. As pointed

[1] Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

out in the White Paper, financial crime-related Regtech solutions are considered the most mature, with a large portion of surveyed banks currently using or implementing Regtech in this area. To facilitate AML/CFT Regtech adoption, the HKMA hosted the AML/CFT RegTech Forum in November 2019[2] to boost awareness of the potential of Regtech in this space. In addition, the HKMA dedicated the Regtech Watch Issue No.3[3] to AML/CFT use cases and published "AML/CFT Regtech: Case Studies and Insights"[4] in January 2021 to share six case studies and thematic insights from the experiences of early adopters. This placed stronger emphasis on key dependencies for Regtech adoption, including securing management buy-in, forming cross-functional and interdisciplinary teams, and data readiness. This Guide supplements that publication with a focus on the use cases of ongoing monitoring of customers. Furthermore, the Guide provides a general framework for the implementation of Regtech within the AML/CFT context, which could provide a better roadmap to adoption.

The use cases of ongoing monitoring of customers were specifically chosen given that industry challenges persist in continuing to balance know-your-client management after onboarding with maintaining a positive customer experience of the bank and meeting regulatory expectations. These considerations have been encouraging a number of banks to implement AML/CFT Regtech solutions. Careful consideration of a number of factors is required for solution implementation to deliver the promised value. Some examples in this Guide involve banks that are further along the adoption journey and have already addressed the dependencies which the "AML/CFT Regtech: Case Studies and Insights" publication had sought to address. While these examples may be too advanced for some of the banks, particularly the smaller institutions, they illustrate how more advanced adopters are exploring Regtech solutions and innovating in this space.

## 1.2 Purpose

The purpose of this Guide is to provide an overview of Regtech solutions for managing an organisation's AML/CFT efforts specifically in the area of ongoing monitoring of customers. The Guide outlines the common challenges observed regarding AML/CFT Regtech adoption, and shares information on how others have successfully addressed the challenges to successfully adopt AML/CFT Regtech solutions.

Ongoing monitoring of customers has been selected as the focus area as it appears to be a less mature area within AML/CFT for Regtech adoption. Many operational challenges in this area are caused by manual processes in collating relevant, complete, and up-to-date information in relation to customers and their transactions. This information is essential to understand if the purpose and intended nature of the customer's activities are commensurate with their risk profile and the nature of the business relationship. The adoption of more advanced technologies such as machine learning and cognitive solutions is nascent. Therefore, these are prime growth areas that could benefit significantly from increased Regtech adoption. As with many use cases for Regtech adoption, there is an underlying assumption that the banks have appropriate processes to capture, classify, store and use data. The ability of a bank to adopt Regtech solutions in the area of ongoing monitoring of customers is dependent on its data infrastructure and underlying data quality.

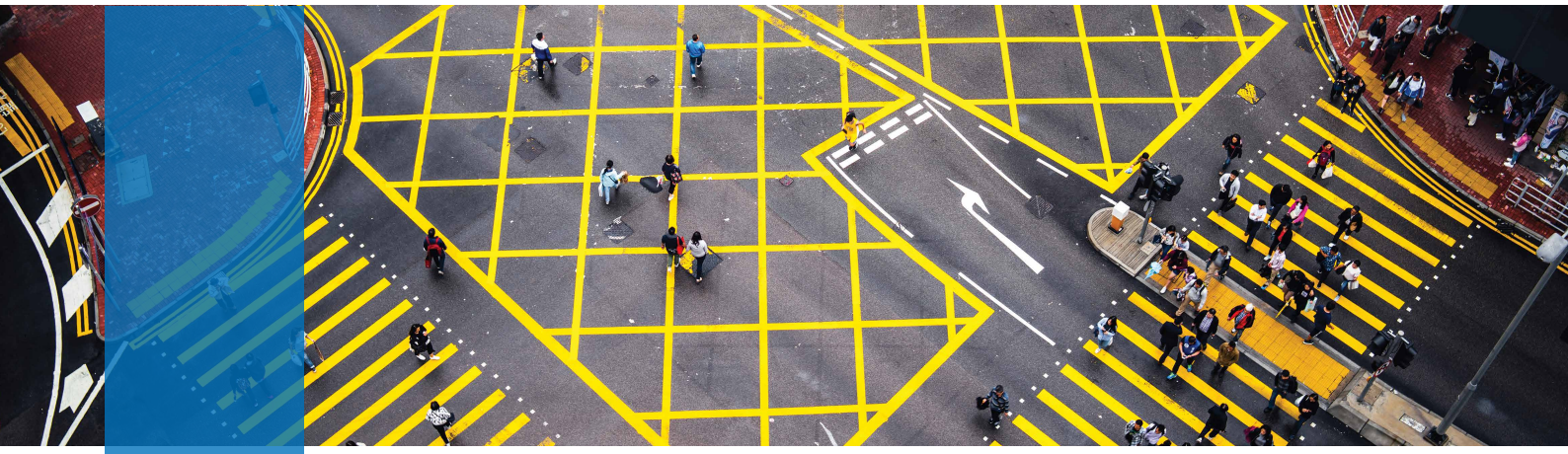
This Guide follows the outline below:

1 **Introduce commonly observed challenges and developments in the ongoing monitoring of customers**
   - Outline the most common challenges and pain points in this area which the adoption of Regtech could help address
   - Outline some of the developments seen in the industry and possible applications of Regtech solutions
   - Describe the key considerations for adopting Regtech solutions for the ongoing monitoring of customers

2 **Provide practical implementation guidelines to banks on the adoption of AML/CFT Regtech solutions**
   - A conceptual framework for Regtech implementation and key considerations when adopting Regtech for the ongoing monitoring of customers

3 **Share use cases on adopting Regtech solutions to manage the ongoing monitoring of customers**
   - Describe the challenges faced by a bank and how the Regtech solution helped to resolve these challenges
   - Outline the key factors from successful AML/CFT Regtech implementation, from both the bank and the Regtech provider's perspectives

[2] HKMA AML/CFT RegTech Forum Record of Discussion, HKMA (December 2019), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191223e1a1.pdf
[3] Regtech Watch Issue No.3, HKMA (June 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200612e1a1.pdf
[4] AML/CFT Regtech: Case Studies and Insights, HKMA (January 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf



# 02 Ongoing monitoring of customer relationships

## 2.1 Key challenges

**Ongoing monitoring of the business relationship with a customer comprises the regular review of customer information and documentation (also known as ongoing customer due diligence (Ongoing CDD)) and the monitoring of customer transactional activity. Ongoing CDD requires the collation of relevant, complete, and up-to-date information in relation to customers and their transactions, which is predominantly a labour and resource-intensive undertaking. Determining whether or not an activity is commensurate with the profile of the customer is not only dependent on the accuracy of data and information available, but equally important is knowledge of the customer's business strategy and intended purpose of the relationship. At the level of transaction monitoring, ensuring that potentially suspicious transactional behaviour and patterns the institution processes are detected for review and scrutiny while managing the volume of alerts is a well-documented challenge that is partially caused by known limitations of rule-based transaction monitoring systems.**

To improve the effectiveness of ongoing monitoring processes, the adoption of one or more Regtech solutions may address challenges in one or both of these areas.

### 2.1.1 Ongoing CDD

Ongoing CDD refers to the review of documents, data, and information relating to the customer which takes place periodically to ensure that they remain relevant and up-to-date. Ongoing CDD for high risk customers is typically performed at a minimum on an annual basis, whereas the frequency for CDD review of non-high risk customers tends to be based on the institution's risk appetite and may be dependent on the customer type, background, and products or services.

In addition to the Ongoing CDD reviews that take place periodically, specific events defined by the institution to have an impact on the customer's risk profile (also known as a trigger event) could also prompt a CDD review of the customer.

#### Challenges

**Heavy manual workload in performing CDD reviews:** Ongoing CDD reviews require manual processing as information relevant to the CDD reviews may still predominantly exist in physical file formats that are not machine readable. Where relevant information in relation to a customer is stored in systems, determining which information source holds the most accurate information in

respect of a customer requires careful evaluation. Analysts spend a lot of time collating information from various information sources to identify where gaps exist and determine whether more current or complete information is necessary for the review.

**Negative customer experience:** Cooperation from the customer is necessary to obtain up-to-date and relevant information, data, and/or documents. Depending on how customer outreach is conducted, customers may find the experience negative and refuse to provide relevant information or delay their cooperation.

**Reliance on customers' notification of changes:** Institutions may not become aware of changes in the information, data, and documents that could affect the customer's risk profile until the customer informs the institution of such changes. Institutions may be prevented from applying the appropriate risk mitigating measures to customers whose money laundering/terrorist financing (ML/TF) risks have increased as a result of such changes, for example if the customer has become a close associate of a person that is entrusted with a prominent public function.

**Challenges in optimising the use of data related to the customer in its totality:** Due to functional silos, information regarding the customer's activities could be handled within the functions without effective sharing of information at the customer level. For example, the fraud monitoring and money laundering activities monitoring teams each perform a review of transactions from their respective investigative angles; the credit risk and the CDD teams each review the customer's risk profile from their respective risk angles, but due to functional silos there may not be a systematic exchange of intelligence that could enhance the overall understanding of the customer.

## 2.1.2 Transaction monitoring

Transaction monitoring is typically performed by automated systems with defined rule-based scenarios that generate alerts based on whether a customer's transactional activity exceeds certain thresholds or exhibits a particular pattern. Alerts generated by the system are then manually reviewed by transaction monitoring alert investigators, who – based on the review of supporting customer information and transaction history – come to a decision as to whether an alerted transaction is suspicious.

### Challenges

**Rule-based monitoring is limited to the rules defined:** Since most institutions rely on clear-cut transaction monitoring rules to generate alerts of potentially suspicious transactions, institutions' ability to identify suspicious activities is often restricted to known money laundering typologies based on which rules are created, and specified data sets that are analysed against those rules. Detecting emerging methods of money laundering, patterns that deviate from defined rules, and complex unknown networks of criminal actors can be challenging with conventional monitoring approaches.

**Challenges in segmenting customers:** To effectively identify transactions that are of an unusual pattern or unusually large in amount, banks are required to assess what is considered as usual. Customer segmentation – where customers are grouped based on high-level characteristics such as entity type, business line, and products used – works on the premise that such shared characteristics will result in similar transactional behaviour so any dissimilar behaviour could be considered unusual. The use of such coarse characteristics for segmentation often sacrifices granularity in favour of simplicity, with dissimilar groups of customers placed in the same segment based on that limited set of characteristics with no strong correlation to transactional behaviour. As a result, thresholds are set based on the aggregate distribution of the segment, resulting in excessive alerts for customers at one end of the distribution and under-monitoring of customers at the other end.

**Challenges in designing scenarios:** Although clear regulatory expectations in relation to the considerations for establishing and assessing transaction monitoring systems are in place,[5] most systems' reliance on specified rules and thresholds pose challenges to banks in ensuring that scenarios are appropriate and balanced across various transaction types and patterns. Differences across scenarios often result in alerts being disproportionately concentrated in particular transaction types, with low alert numbers or even no alerts for other transactions. One of the limitations of a rule-based approach is that it is only able to monitor what is already known. If the design or coverage of existing scenarios is insufficient or overlooks certain behaviours of a specific customer segment or with respect to a certain transaction type, there is no way for the system to identify such gaps.

[5] Guidance Paper, Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting, HKMA (May 2018), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180510e3a1.pdf

**Challenges in setting and maintaining scenario thresholds:** For transaction monitoring scenarios to operate effectively, thresholds must be set at reasonable values relative to customers' actual activities and must be reviewed and revised (as appropriate) on an ongoing basis to ensure that thresholds remain appropriate as activities of customers change. Banks often face challenges with the adoption of one set of thresholds and parameters across multiple different customer segments, or outdated thresholds and parameters that have not been properly reviewed and tuned. Improperly set thresholds and parameters (in general, and in relation to specific customer segments) may lead to the accumulation of excessive alerts or under-monitoring where suspicious activities may go undetected. When banks do initiate a threshold tuning exercise, there is often a large cost and time investment associated with transforming an appropriate tuning methodology into actionable results.

## 2.2 How can AML/CFT Regtech solutions help?

AML/CFT Regtech solutions can address the challenges related to the ongoing monitoring of customers by digitalising customer and transactional data, mimicking existing research and investigative processes of analysts to organise information by relevance for an optimised review of information, or by providing insights that are withheld from conventional approaches due to system limitations. However, the effective operation of any of these AML/CFT Regtech solutions requires a certain level of data quality, which requires institutions to have in place proper governance and data processes covering the collection, preparation, storage, and distribution of data to ensure that it is reliable for statistical calculations and insights. The following section, while not exhaustive, outlines several applications of Regtech to illustrate the possibilities that banks may explore in these areas. **Section 4** of this Guide sets out three use cases which have been selected based on considerations such as the relevance of solutions used to address the challenges mentioned in **section 2.1**, the impact on a bank's current operating model, and whether a use case would be fit for the purpose of this Guide.

### 2.2.1 Ongoing CDD

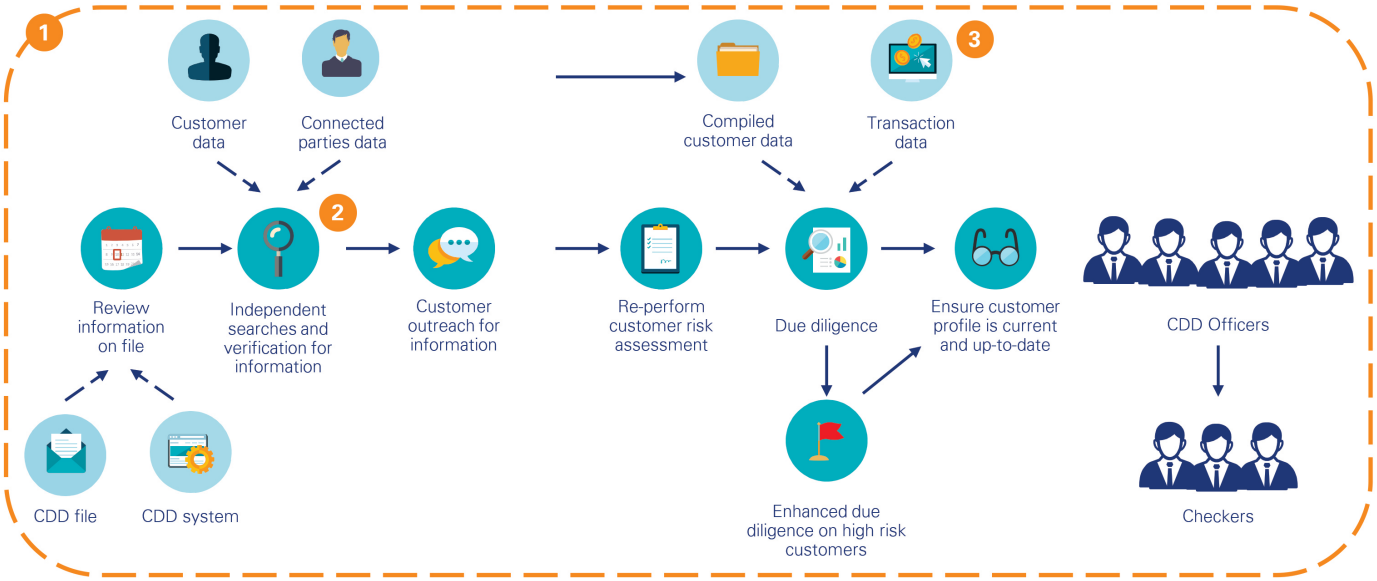
Figure 1 illustrates the possible solutions that may be implemented to tackle pain points related to Ongoing CDD.

1) An integrated technology platform incorporating intelligent workflows and automation capabilities to reduce manual activities in CDD; and a customer interface that enables customers to provide and manage data which is relevant to customers

2) Cognitive computing solution that performs searches, categorisation, filtering, and analysis of financial crime information about the research subject (e.g. customer)

3) Analytics and visualisation in customer activity review to enable a more integrated approach to monitoring

Figure 1: Potential solutions for Ongoing CDD

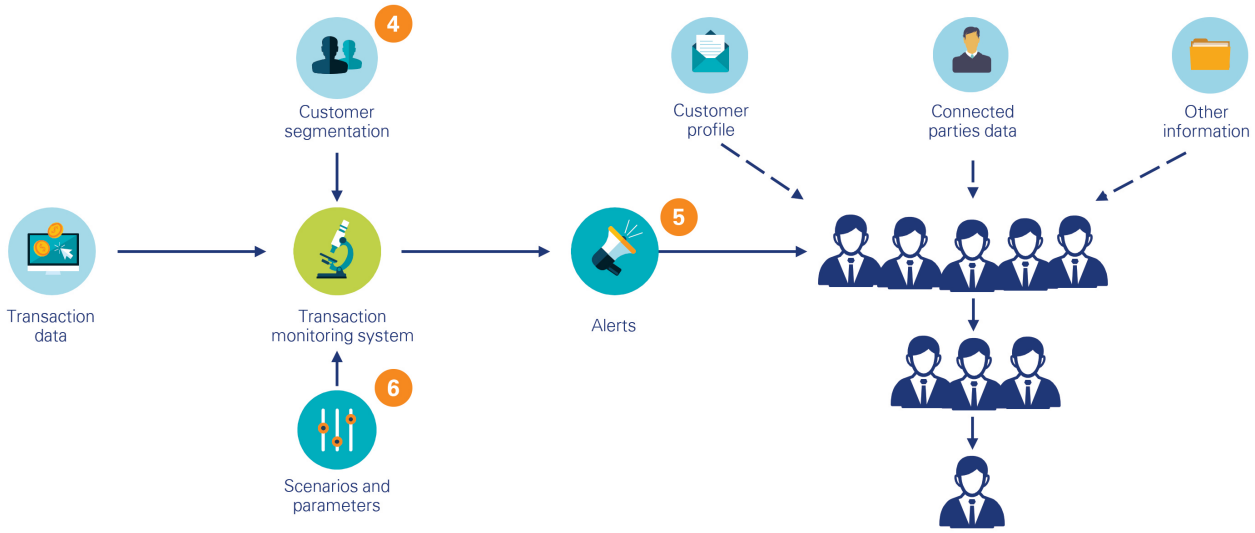



Source: KPMG

## 2.2.2 Transaction monitoring

Figure 2 illustrates the possible solutions that may be implemented to tackle pain points related to transaction monitoring.

Figure 2: Potential solutions for transaction monitoring




Source: KPMG

4) Machine learning-powered customer segmentation

5) Machine learning for transaction monitoring alert classification to alleviate the heavy manual workload in reviewing large quantities of alerts and heavy reliance on experience and judgement in the initial levels of review

6) Robotic process automation (RPA) in transaction monitoring threshold tuning to address challenges in setting and maintaining scenario thresholds

*Other transaction monitoring Regtech solutions include network analytics which has been covered in detail in the HKMA's "AML/CFT Regtech: Case Studies and Insights"[6] and RPA solutions which increase the efficiency of investigations.

[6] AML/CFT Regtech: Case Studies and Insights, HKMA (January 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf

## Solution 1: Integrated technology platform

To address the heavy manual workload in performing CDD reviews, an integrated services technology platform that is set up with an intelligent workflow can address various challenges faced by institutions. Customer data can be digitalised and loaded onto the platform for the identification of information and documentation gaps. This is an important step in ensuring data readiness for future use as not only does it establish a data collection and processing process for future consistency and completeness, it also ensures the proper storage and accessibility of data for different uses. The platform could offer a solution to engage with customers digitally which can address challenges faced by institutions in relation to managing the customer experience. With the digitalisation of customer information and data, management information reporting and analytics can be developed in time to provide insights into trends and changes in customer segments.

## Solution 2: Cognitive computing research solution

Supervised machine learning techniques may be applied for the aggregation of information from public and subscribed data sources and the open web for the purposes of performing searches, categorisation, filtering, and analysis of financial crime information about the research subject (e.g. customer). Machine learning models can learn from historical searches and decisions made by analysts and make decisions on alert outcomes based on the data available. These applications of machine learning to support human decisions pair well with natural language processing (NLP), which would allow a solution to assess the content, extract relevant information, eliminate false-positives and deduplicate content into a single thread, and classify information by threads. While this should not act as a complete replacement for human review due to the risks involved, machine learning could be used to provide an initial grouping of information by relevance before human review so that a decision can be made more quickly with adequate support. The solution can also generate alerts to event-driven changes in the customer risk profile, which helps to meet the need for accurate and up-to-date information. See use case #2 for more information.

## Solution 3: Analytics and visualisation in customer activity review

Transaction monitoring alerts are often investigated at the transaction level, with investigators lacking a holistic view of customer activity in all of the customer's accounts and related parties' accounts due to a lack of integration between multiple systems and data sources. Regtech can be applied to address this by integrating data from multiple sources, applying advanced analytics techniques, and visualising results comprehensively to highlight activities of the customer that deviate from normal patterns and behaviours. This integrated approach may bring together multiple techniques/core technologies such as RPA and machine learning, with the focus on generating a visual output in the form of a comprehensive dashboard that communicates data insights to the investigator. See use case #3 for more information.

## Solution 4: Customer segmentation using supervised machine learning

Placing dissimilar groups of customers in the same segment often leads to ineffective threshold setting and a high number of false positives. One avenue that is being explored is the use of supervised machine learning techniques to cluster customers based on a more granular combination of data points including demographic or entity-specific information and their historical transaction patterns. Each cluster is assigned a threshold calibrated based on their transaction activities. By using machine learning to facilitate more granular segmentation, existing scenarios can be made more effective and lead to a reduction in false positives. Use case #1 provides details on the results of a proof of concept (POC) of the solution.

## Solution 5: Machine learning for transaction monitoring alert classification

Supervised machine learning techniques may be applied for classifying alerts and detecting those that do not require further manual review. Machine learning models can learn from historical data on human decisions and make decisions on alert outcomes based on the data available, reducing the human input required to close an alert. While this should not act as a complete replacement for human review due to the risks involved, machine learning could be used to provide an initial assessment and rationale before human review so that a decision can be made more quickly with adequate support. These applications of machine learning to support human decisions pair well with natural language generation (NLG), which would allow a solution to generate human readable justifications for decisions.

## Solution 6: RPA in transaction monitoring threshold tuning

Keeping a transaction monitoring system effective over time requires regular calibration of thresholds. Many banks do not have a well-established process for regular threshold tuning, with high alert volumes and poor quality alerts as results. Some banks have implemented RPA solutions to partially automate the threshold tuning process, for example the processing and analysis of the performance of the rule settings according to the bank's prescribed tuning methodology and running analysis of above-the-line and below-the-line testing to calibrate thresholds and parameters. This reduces the manual workload and risk of errors involved in carrying out tuning manually, and allows for more efficient and frequent tuning of system thresholds.

## 2.3 Key considerations for adopting AML/CFT Regtech solutions

Similar to the adoption of Regtech in other application areas, budget and resource constraints are typically the main considerations when planning the implementation of an AML/CFT Regtech solution. According to the White Paper,[7] 75% of surveyed banks expressed that "budget or resource constraints or an unattractive business case" was one of the top five barriers to Regtech adoption, with a lack of capabilities among existing staff also cited as a key concern.

To address budget considerations, institutions may take measures prior to implementation to ensure that resource needs are met and the business case for the solution is well articulated. This may involve conducting a thorough cost/benefit analysis to determine the return on investment, including estimating the long-term cost savings from investing in the solution. It may also be useful to map out key stakeholders within the organisation and determine the key individuals that should be engaged to ensure that the project has the necessary financial and management buy-in.

When considering capabilities among existing staff, banks should first assess the required skills for project implementation, and evaluate where the corresponding capabilities may exist within the wider organisation, including the possibility of canvassing skills from other teams, departments, or related entities such as group IT. Even if a gap in capabilities within the organisation is identified, this should not be considered the end of the exploration; the bank may evaluate options, such as redeveloping existing resources with competencies to acquire new skillsets, considering short-term specialist hires, or collaborating with an external party, and weigh the investment against the estimated long-term benefits of implementation.

[7] Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf

In addition to these general considerations, ongoing monitoring of customers comes with specific considerations and risks, which are outlined below.

**Data quality and availability:** The success of any AML/CFT Regtech solution hinges on the availability of high quality data. Transaction monitoring processes require data inputs from multiple sources, which may create data integration challenges if there is not a single source of truth (or "golden source") for data. Different functions within the same organisation may also have differing levels of data infrastructure and technological maturity. There may be a reliance on manual data processing and non-digitised information collation at key junctures (e.g. certain customer profiles that exist only in paper form) which creates barriers to implementation at scale.

**Compatibility with existing systems:** Most institutions' systems for transaction monitoring are either sourced from an external vendor or developed in-house. Systems are often programmed to run a specific process end-to-end, making the Regtech solution's compatibility with existing upstream and downstream systems crucial.

**Risk of implementing "black-box" processes:** The results of investigations and the processes used to arrive at such results must be transparent and auditable. This is of particular concern for machine learning applications where the inner components or logic cannot be inspected.

**Risk of quality lapses:** Existing AML/CFT processes often employ multiple layers of controls to reduce the risk of missing potentially suspicious activity, designated persons or entities, such as four-eye checks. In replacing or enhancing these existing processes, there is often an impetus to demonstrate that the Regtech solution performs at least as well as the experienced and knowledgeable staff. This means that institutions may be required to continue running existing processes in parallel with the newly implemented technology solution, or implement additional quality assurance reviews to confirm the solution's output is as robust as when performed by staff.

# 03 Implementation guidance

**While the set of processes and controls within AML/CFT applications are largely well defined, there is a great breadth of possible Regtech solutions that may be implemented to enhance these processes, allowing organisations to explore a wide range of core technologies.**

Due to the wide array of core technologies available, particular consideration would be required depending on the characteristics of the technology that a bank wishes to implement. A key consideration is data readiness, a topic well-covered in the "AML/CFT Regtech: Case Studies and Insights"[8] in January 2021. This section does not intend to provide an exhaustive guide to implementation of a technology. Instead, it outlines a general framework for implementation within the AML/CFT context.

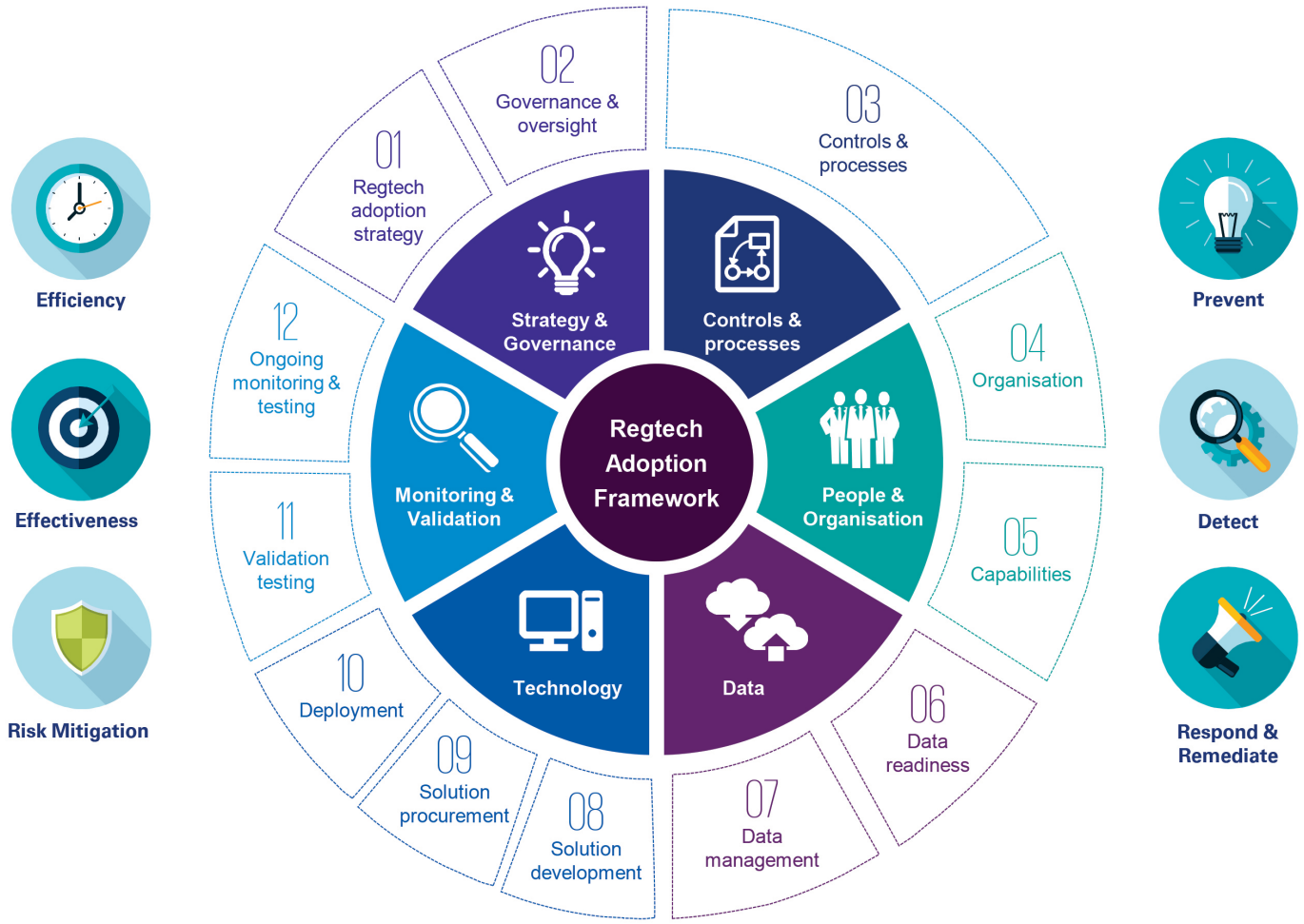
## 3.1 Regtech adoption framework

Most banks that have adopted Regtech to date have not followed a set framework for adoption. Adoption has usually taken the form of a use case-led or solution-led approach, i.e. starting with a specific business problem or risk outcome and identifying a suitable technology to address this end goal, or starting by investing in a particular core technology or solution that could be applied to generate a range of downstream benefits across multiple use cases.

[8] AML/CFT Regtech: Case Studies and Insights, HKMA (January 2021), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf

Irrespective of the approach, an adoption framework could provide better structure to the adoption journey, enabling institutions to better understand the current state, particularly in relation to current processes, data readiness, and management; what it envisages for its future state; and map out what it needs to achieve this future state, for example oversight mechanisms and key success factors and ongoing monitoring of the solution. An adoption framework is proposed in Figure 3:

Figure 3: Regtech Adoption Framework




Source: KPMG

Regtech adoption may not follow a defined strategy or may be prompted by a specific business objective, risk outcome, or pain point. A bank should consider whether a solution is able to achieve objectives across key drivers such as enhanced efficiency, improved effectiveness, strengthened risk mitigation capabilities, or an improved customer experience. A bank should also consider whether the solution enhances the bank's capabilities to prevent, detect, or respond to money laundering and terrorist financing activities or remediate deficiencies in AML/CFT controls.

The adoption framework covers considerations across relevant aspects of the adoption process and evaluates a bank's readiness across key areas. It is largely applicable to the adoption of any AML/CFT Regtech solution, regardless of the underlying technology.

Figure 4 maps out an adoption journey that a bank can consider, whether the starting point is use case-led or solution-led, and ensures that all relevant components of the aforementioned adoption framework are considered.

Given majority of the framework had been covered by various HKMA AML/CFT publications (full list please see the Appendix A.2), this Guide will deep-dive into some key elements in "Technology", "Validation testing" and "Ongoing monitoring".

### 3.1.1 Technology

Where the implementation is driven by a use case, banks may begin with a technology agnostic approach and explore multiple core technologies that are capable of addressing the problem statement. To evaluate whether a potential technology is suitable, a bank may consider factors such as:

- Does the technology sufficiently address the problem?
- Is the technology appropriate for the scale, business and technological maturity of the organisation?
- Is the complexity of the technology commensurate with the complexity of the problem?
- Is the technology compatible with the existing environment?
- Does the technology align with a future technology roadmap or the agreed architectural principles?
- Are there sufficient capabilities to develop this technology? (either within the firm or with suitable third-party vendors)
- Is the technology robust enough for the future?

Banks should also ensure that the technology fulfils certain criteria:

- **Auditability:** To enable review, banks should produce proper documentation outlining the logic used by the solution. This documentation should be updated regularly. Sufficient audit logs should be built during development stage and should be retained for an appropriate period of time to ensure auditability.
- **Explainability:** For solution outputs to be sufficiently trustworthy to support AML/CFT processes, the solution's decisions must be explainable. During design and development stage, banks should make efforts to include explainability as a core component. In the two use cases described in **section 4** of this Guide where machine learning was applied to support decisions, special efforts were made to build-in explainability as a core functionality by programming the solution to output human-readable rationales outlining the key deciding factors.
- **Resilience:** AML/CFT solutions often draw data from multiple sources and are thus widely exposed to changes in data or systems. If a bank is exploring a solution that requires ongoing data collection (e.g. RPA), it should take measures to future-proof the solution. This may involve putting in place measures to boost resilience, such as prioritising modularity (i.e. building the solution in separate components so that one piece can be replaced without affecting others) and implementing robust error handling logic.

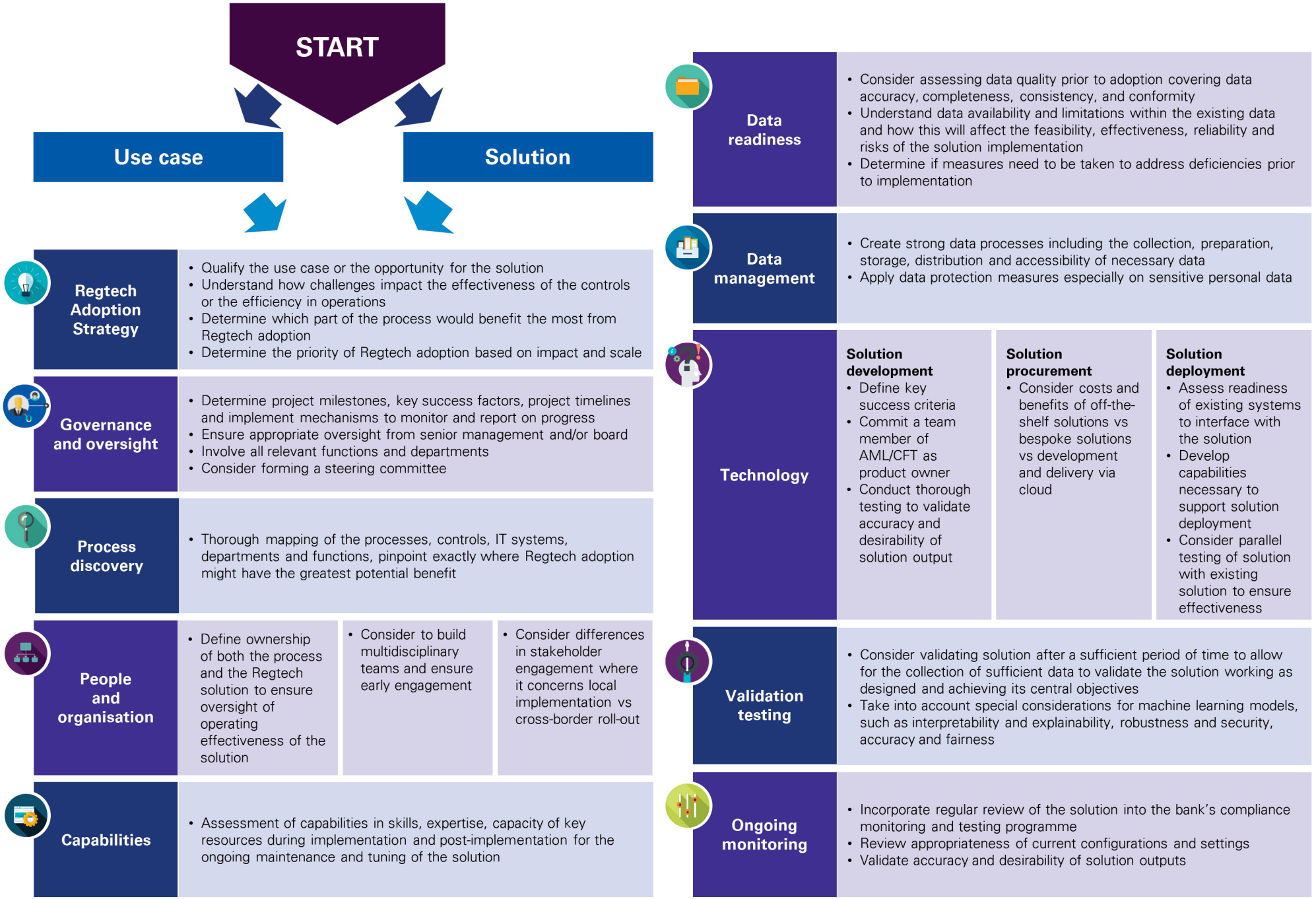
### 3.1.2 Validation testing

The central goal of validation is to assess whether the solution is working as designed and is generating the output or results for which it is designed to meet its key objectives. The bank should consider performing a validation review after a sufficient period of time of operation (e.g. one year after implementation) to allow for the collection of enough data to reliably validate effectiveness. The validation may involve an end-to-end review of the model, its performance and operating effectiveness to identify any issues that may be impairing effectiveness, for example poorly calibrated parameter settings, system errors or data integration issues. The bank may then evaluate the reasonable actions required to address the issues identified. In addition to ensuring the effectiveness of the solution in question, identifying common challenges and key learnings through comprehensive validation exercises can also be beneficial in developing capabilities and deriving best practices for future Regtech implementations.

### 3.1.3 Ongoing monitoring

Due to the dynamic nature of customer activities based on which machines are trained to identify patterns or clusters, ongoing testing is important to ensure that the solution is performing as expected. The performance of Regtech solutions should be reviewed on a regular basis, with testing procedures and frequency stipulated in the bank's compliance monitoring and testing plan. The bank may also consider performing updates and testing in response to events that may materially affect the solution's performance or functionality (e.g. changes to regulations, changes to the bank's systems or data infrastructure, or the introduction of new products, channels or business lines for which the same logic cannot be applied). Regular testing should cover the solution's performance criteria defined. Where key performance criteria are not met, the performance lapses should be investigated and addressed at once.

Figure 4: Sample AML/CFT Regtech adoption journey



# 04 Regtech use cases

## 4.1 Use case #1 – Machine learning powered customer segmentation

**Leveraging machine learning technology for more precise customer segmentation, the POC for this solution was able to enhance the effectiveness of the scenarios in a bank's transaction monitoring system, which led to a reduced number of false positives.**

### Challenge

The significant volume of transaction monitoring alerts combined with other AML/CFT controls processes such as periodic CDD reviews systematically stretched the capacity of the relevant teams at the bank. In an effort to more accurately identify transactions that may lead to the filing of a suspicious transaction report (STR), machine learning was identified as a core technology that could be applied to enhance efficiency.

### Approach

A solution-led approach was taken with machine learning identified as the technology to be explored due to successes observed from industry peers, and various applications were considered. The bank considered two options: a model that would facilitate the identification of suspicious transactions by introducing new customer segments; or a model that would review the alerts generated by the current rule-based transaction monitoring system. The bank chose the former. With the help of an external vendor, a supervised machine learning model was developed to identify clusters of customers based on a broader range of characteristics, including demographic, geographic, transactional, and behavioural data within the organisational segments customers had been assigned to (e.g. retail banking and corporate banking).

### Benefits

The supervised machine learning model was able to identify new customer clusters, on which new thresholds could be calibrated by referencing historical transaction

patterns while ensuring that alerts that resulted in STR filings could be identified under the new thresholds. This refined customer segmentation resulted in better scenario performance and therefore improved the effectiveness of the rule-based system, while achieving a 50% reduction in the volume of alerts generated by the transaction monitoring system.

## Key success factors

- **Forward-thinking mindset from subject matter experts:** Governance over the project was led by the head of compliance and head of Financial Crime Compliance (FCC), both of whom had a forward-thinking mindset and were keen to explore Regtech options, which was key to securing buy-in and funding for the solution. To provide oversight of the project, bi-weekly update meetings were held between the vendor and the bank's head of compliance and head of FCC to provide updates on progress and interim results of the solution. Success criteria were set collaboratively between the bank's stakeholders and the vendor at the beginning of the project, with progress against those criteria reported regularly. The importance of a "just do it" mindset was highlighted in getting the project off the ground.

- **Careful prioritisation:** In the consideration of the options of adopting machine learning, this bank considered the value in the longer term and where a more direct positive impact could be achieved.

- **Clear roles and responsibilities:** The implementation was owned and led by the FCC team, with internal IT involved in an auxiliary support role. Ultimate ownership for the success of the project was shared between the parties and a careful plan outlining the various work activities between the parties also ensured the measurability of progress to senior management.

- **Using external expertise:** The bank examined its own internal capabilities and concluded that an external vendor would be able to provide additional technical expertise that could not be easily sourced internally. In bringing in external capabilities, the bank also used the implementation as an opportunity to enhance its own staff's capabilities, with knowledge transfer conducted throughout the project. A member of the bank's staff with a data background liaised with the vendor day-to-day and gained exposure and knowledge of the solution's underlying technology.

- **Key success criteria had been defined and met:** Instead of setting quantitative success criteria, the parties collaboratively agreed that the criteria to evaluate the success of the POC required the consideration of various dimensions, including whether or not alerts that resulted in the filing of a STR could be identified, whether new thresholds set for each customer segment could be supported with adequate rationale, and whether a meaningful reduction in the volume of false positive alerts could be achieved.

- **Quality of test data:** While data quality was important, it was not thought of as a potential barrier to developing a machine learning solution, as developers identified that the level of data required for proper conventional transaction monitoring would also fulfil the needs of a machine learning model. In this particular case, the development leveraged the availability of an existing transaction data set that was used for the model validation of the transaction monitoring system, which met the requirements for model development. Although data quality was validated at the beginning, data completeness issues were discovered in the middle of development; a key learning point is to involve subject matter experts who have an understanding of the expected data for normal business operations and can resolve the data issues during development in addition to conducting more systematic validation checks.

- **A model-agnostic approach** was taken during solution development. Multiple machine learning models were explored, and the optimal model was decided to be adopted based on statistical metrics. A wide range of hyperparameters[9], features, and dimensionality reductions were also explored during the model tuning process.

- **Ongoing testing plan:** A plan was designed to validate and fine-tune the model on an ongoing basis by integrating below-the-line testing into the transaction monitoring process. A sample of below-the-line alerts would be randomly generated and reviewed "blind" by bank investigators, enabling the continuous collection of new data to validate and retrain the model.

[9] Hyperparameters are parameters that can be used to control the model training process.

## 4.2 Use case #2 – Cognitive computing research solution

**A machine learning-powered real-time research solution that performs research on the subject through corporate records, sanctions, regulatory watchlists, adverse media, and web screening against a vast amount of open and subscribed sources. Replicating the cognitive and investigative process of a due diligence analyst through the application of machine learning and cognitive computing, relevant information is identified and highlighted for review.**

### Challenge

Periodic review of backlogs stretched the capacity of the CDD operations of a bank. Analysts spent a lot of time researching changes to the customer and/or its related parties that would raise the ML/TF risk profile of the customer. Accordingly, the bank was exploring if technology solutions were available that could perform these searches and alert the bank if there were changes to the customer's risk profile. If the solution proved to be reliable over time, the bank could consider at a future stage to revisit the periodic review cycle for at least its non-high risk customers.

### Approach

The overall objective of the bank was to explore if a solution was available that would reduce the research time for analysts and enhance analysts' ability to identify changes that indicate a change in the ML/TF risk profile of the customer. The bank engaged a third-party vendor and was provided with two options: a self-service platform which the bank could use to run searches and adjudicate search results; or a fully-fledged service by the third-party vendor where the vendor would run searches on behalf of the bank with the solution, adjudicate search results and deliver research reports to the bank. The bank decided on the first option.

### Benefits

The solution replaced the manual research and investigations of the customer and reduced the time CDD analysts spent on researching whether there is information in relation to the customer that would change the risk profile of the customer. The research covered the abovementioned categories of information and therefore replaced the individual screening processes. As information was organised into threads through NLP in over 25 languages and auto-translation from over 60 languages, the accuracy

of results significantly improved, eliminating close to 95% of false positives. In addition, continuous monitoring automated by the solution ensured event-driven reviews were initiated in a timely manner.

## Key success factors

- **Effective communication and training:** There were rounds of discussions between the bank and the third-party vendor to understand the bank's expectations and requirements in order to better customise the solution for the bank. Implementation discussions and trainings were held to assist in-house analysts in using the solution and communicate technical requirements such as file formats required for batch uploads.

- **Collaborative approach on design:** Prior to the implementation of the solution, the bank's head of FCC and head of IT had explored the solution and the flexibility of the design as well as more specific matters such as the location of the Cloud and IT security with the vendor. The ultimate decisions were captured in the design of the tool in accordance with the bank's preferences and risk appetite, such as risk categories, risk weightings, search terms used to identify key risks, ultimate beneficial owner threshold, and the fields brought back under the corporate record. As such, the solution could better address the specific third-party risks faced by the bank.

- **Transparency in the design and operation of the matching algorithm:** The solution used fuzzy matching in its searches to allow for common name synonyms, misspellings against structured sources, and dialect variations. It also had a feature to recommend common variations and transliteration variations of names using a variety of sources, including spell checking and transliteration engines. Users of the solution could slide the level of fuzzy matching along a scale to bring in more or fewer results and filter them using its association scoring and event classification. All search records along the fuzzy matching sliding scale were still captured and available for viewing should the analysts require. This would also mitigate the risk of mistyping by analysts and address issues associated with the transliteration of names from different languages.

- **Business as usual (BAU) trials:** BAU trials were run prior to adoption of the solution. The third-party vendor took a sample of the third-party population that the bank had selected, with a range of varieties in terms of risk, size, type, and location, and processed the sample with the solution, then compared the findings against the

bank analysts' findings. Conducting BAU trials increased the bank's confidence in the operating effectiveness of the solution, specifically as to whether gaps had been identified as compared to manual searches, as well as realising efficiency gains from adopting the solution and facilitating subsequent implementation.

- **Dashboard reporting via performance analytics:** The bank had also deployed a solution to manage the end-to-end workflow which further enhanced the efficiency in the due diligence tasks performed by in-house analysts. The workflow solution supported the bank in identifying and capturing issues, actions, and remediation, as well as managing and tracking actions to completion. The effectiveness of the due diligence solution in reducing the time spent on each case could be quantitatively measured with the workflow solution.

- **Scalability:** The maximum number of searches to be handled concurrently was configured to best suit the bank's needs. The third-party vendor communicated with the bank to determine the number and type of searches (e.g. small local vs large multinational). Additional crawlers could be added to expand capacity when needed.

- **Ongoing testing plan:** A plan was designed to validate and tune the model on an ongoing basis. The solution used a supervised learning process to control the learning outcomes, as opposed to unsupervised learning. The third-party vendor manually reviewed discrepancies in adjudications and modified the training process accordingly.

## 4.3 Use case #3 – Customer activity dashboard

**Integrated approach bringing together multiple techniques/core technologies such as RPA and machine learning, with a focus on generating a visual output in the form of a comprehensive dashboard that communicates data insights to the investigator.**

### Challenge

As part of its Ongoing CDD, a bank required the review of each customer and their related accounts' transactions on an aggregated basis to evaluate if there were indicators of patterns or behaviours that were not commensurate with the bank's understanding of the customer. For this review, the bank was required to gather data from multiple systems as the transactions covered all relevant transaction types the customer engaged in. The bank was faced with the challenge of generating insights from the transactional data.

### Approach

A two-step approach was adopted to provide the bank with useful insights to determine whether the customer's transactions were commensurate with the bank's understanding of the customer's risk profile. First, the bank implemented a RPA tool with the help of an external party, who developed the solution on-premises. The tool reduced the effort in collating the information from various systems by replicating and automating the existing data processing procedures. Other non-transactional information (e.g. the opening of a new account, login details, and locations) were added to the database. Thereafter, customer activity displaying red flag indicators were identified and visualised in a dashboard giving insights into transaction patterns indicative of ML/TF, as well as geographic and counterparty clusters, through which the bank was able to detect activities that were not in line with the profile the bank had of the customer. The bank has proceeded to explore the development of a machine learning model to identify transactions that were unusual in comparison with the customer's other data.

### Benefits

In addition to being able to generate useful insights into the customer's transactions and better understand the customer's transactional behaviour to determine if these were commensurate with the bank's understanding of the customer, the solution ensured that available datapoints were aggregated and reviewed holistically at the customer level. The visualisation tool could be customised in line with the risk view specified by the reviewer.

## Key success factors

- **Effective communication:** There had been rounds of discussions between the bank and the third-party vendor to understand the bank's expectations and requirements in order to better customise the solution for the bank. The discussion covered not only the areas of subject matter expertise, but also the users that would benefit from the investment and involved the local and regional heads of the division, the first-line risk management function, the operations function, local and regional head of FCC, head of compliance for monitoring and testing, and head of internal audit. The vendor was straightforward with what would be feasible and what would require more work.

- **Key performance metrics:** The bank and vendor had identified key success factors throughout the implementation process. For example, the first milestone of the project was agreeing the risk views and red flag indicators the bank wanted to see and identifying the necessary data points to create the risk views. The next milestone was to ensure that the identified data points were mapped to the source systems and that the source systems could be accessed and the data could be extracted to the central database. By specifying the performance metrics up front, any progress or delays were transparent to all parties and any barriers to reaching them could be addressed in a timely manner.

- **Clear roles and responsibilities:** This bank had dedicated a project team comprising members from the business unit, IT and operations to work alongside the vendor, ensuring that the output from the work met the bank's requirements. A key lesson learned in the process for the bank was to ensure that persons with decision-making authority were assigned to the project team to ensure that the milestones could be met.

- **Capability augmentation:** The bank had internal capabilities with the requisite technical expertise. However, the bank made a conscious decision to work with an external vendor so that the internal team could leverage external practices to augment internal capabilities. This has also helped the bank to identify gaps in technical capabilities and evaluate the expansion of these capabilities in-house.

# A Appendix

## A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Rani Kamaruddin, Paul McSheaffrey, James O'Callaghan, Stanley Sum, Thomas Tsang, Bryan Chan, Rowena Lee, editor Kanishk Verghese

## A.2 Relevant regulatory requirements and/or guidance

| Name | Link |
|---|---|
| HKMA Supervisory Policy Manual – Supervisory Approach on Anti-Money Laundering and Counter-Financing of Terrorism (AML-1) | https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SPM-AML-1.pdf |
| HKMA Supervisory Policy Manual – Outsourcing (SA-2) | https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf |
| HKMA Supervisory Policy Manual – General Principles for Technology Risk Management (TM-G-1) | https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf |
| Feedback from Recent Thematic Review of AIs' Sanctions Screening Systems | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180412e1.pdf |
| Feedback from Thematic Review of the Use of External Information and Data in AML/CFT Systems | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1.pdf |
| Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting (Revised in May 2018) | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20180510e3a1.pdf |

| | |
|---|---|
| Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorised Institutions) | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf |
| HKMA AML/CFT RegTech Forum, 22 and 25 November 2019 – Record of Discussion | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191223e1.pdf |
| Report on "AML/CFT Regtech: Case Studies and Insights" | https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1.pdf |
| Office of the Privacy Commissioner for Personal Data, Hong Kong – Guidance on Personal Data Protection in Cross-border Data Transfer | https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf |